Sistemas de prevención de intrusiones: ¿una nueva tecnología?

En el presente artículo se define el concepto de la prevención de intrusiones –tan de moda hoy– y se abordan las técnicas que se están imponiento al respecto: sistemas operativos bastionados, IDS en línea para cortar ataques... Los autores también intentan dar pautas para distinguir los sistemas de prevención de intrusiones (IPS) de los que no lo son pero se venden como tales.

Antonio Requejo / Javier Fernández-Sanguino

Cada año que pasa nos encontramos en este mundo de la seguridad IT con nuevos términos, conceptos o categorías de soluciones. Y es que a pesar de que los fundamentos sean los mismos que antaño, las aproximaciones a la resolución de los problemas cambia. Este cambio viene justificado por la evolución tecnológica, por los cambios en los modelos de negocio y por qué no, por la necesidad de "vender" nuevos mensajes y diferenciarse la competencia.

Uno de esos nuevos términos, que nos ha llegado a lo largo de los últimos meses, es el de la "prevención de intrusiones". El pasado mes de abril, la prestigiosa cita de la RSA Conference ya contó con un espacio dedicado al tema en su agenda. Cisco ha comprado Okena, Network Associates ha adquirido Entercept e IntruVert Networks, Symantec ha hecho lo mismo con Recourse Technologies, NetScreen también con OneSecure, empresas todas ellas cuyos sistemas de prevención de intrusiones (Intrusion Prevention Systems, IPS) habían tenido una muy buena acogida en el sector.

El proceso de seguridad

Pero, ¿qué es exactamente la prevención de intrusiones? Para responder a esta pregunta hay que considerar cómo se hace (o debería hacer) la implantación de la defensa frente a ataques de seguridad en un entorno organizativo. Bruce Schneier propone [SCHNE200] un sencillo modelo de "proceso de seguridad" basado, exclusivamente, en tres estadios asociados a la seguridad en un sistema: Prevención o Protección, Detección, y Reacción o Respuesta.

Prevención o Protección: en este estado se han implantado elementos que protegen a los sistemas de la organización frente a ataques que puedan producirse, basándose en un correcto análisis de riesgos que ha definido previamente los activos a proteger y las contramedidas a adoptar para protegerse de sus posibles vulnerabilidades. Dentro de los sistemas de prevención se implanta la supresión de ataques mediante la eliminación de la amenaza de forma general, evitando su aparición. Es por tanto una aproximación proactiva, previa a la aparición del ataque en sí mismo. Ejemplo clásico de esta aproximación es el diseño de sistemas para que fallen de forma segura, el uso de puntos de control en una red, la defensa en profundidad y la "compartimentalización".

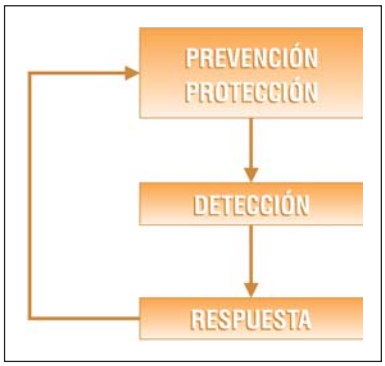

Figura 1.- Proceso de seguridad propuesto por Bruce Schneier

Para responder exactamente a la pregunta ¿qué es la prevención de intrusiones?, hay que considerar cómo se hace o debería hacer la implantación de la defensa frente a ataques de seguridad en un entorno organizativo.

Detección. La detección de ataques se despliega como complemento a las medidas de prevención para llenar los huecos que dejan éstas. Dicho de otra forma, para atajar el nivel de riesgo residual que no pueden rebajar las medidas de protección. Se dota a una infraestructura de medidas de detección porque se asume que las de prevención no son suficientes para atajar todos los ataques, y es necesario saber cuándo las medidas de protección no han sido efectivas.

Reacción o Respuesta. Pero la detección ha de tener siempre el complemento de la respuesta, bien automatizada (con apoyo de un sistema de decisión), bien realizada con intervención humana, es decir, de forma manual. Así, en un caso la salida del sistema de detección será una alerta, enviada a una consola o dispositivo, almacenada o impresa, en el otro, una serie de acciones encaminadas a eliminar o mitigar el ataque. El objetivo final es recuperar el sistema atacado.

IPS dentro del proceso de seguridad

Los primeros productos que fueron apareciendo con la "etiqueta" de *Intrusion Prevention* tenían, como características taxonómicas principales:

– Estar centradas principalmente en la protección local de los activos, acuñándose el término HIP (*Host Intrusion Prevention*).

– Tener una aproximación reactiva, esto es, basadas en Detección+Respuesta, siendo esta respuesta automatizada, bien mediante reglas de configuración, bien mediante la propia "inteligencia" del sistema de HIP.

Esta última característica les diferencia cualitativamente de los sistemas de protección pues las medidas de eliminación del ataque no son aplicadas hasta que el ataque no se produce. En el momento en que se detecta un ataque, se responde eliminándolo. A diferencia de un sistema defensivo que está configurado protegido de ataques antes de que éstos se produzcan.

Por supuesto, estos productos incluían en ciertos casos capacidades de Protección, pues su inclusión es barata tanto en recursos necesarios para dotar de dicha funcionalidad al sistema como en recursos necesarios para su aplicación. Estas medidas de protección pueden ir desde el bastionado del sistema hasta el filtrado de ciertos tipos de conexiones.

La hasta entonces popularización de los medios de protección frente a los medios de eliminación de intrusiones (o ataques) se debió a dos causas, la primera ya se ha mencionado anteriormente, resulta sencillo cubrir un porcentaje de los ataques de forma eficiente en cuanto a recursos mediante esta aproximación. Digamos que hay un gran número de posibles ataques fáciles de detener con medidas estáticas, implantadas de forma previa a su aparición.

La segunda razón es el "riesgo" que conlleva la aproximación de Detección+Respuesta. Como se ha mencionado, esta defensa de los activos se sitúa cerca del propio activo, y por tanto es "nuestra última esperanza". Es algo así como el portero de un equipo de fútbol. Y en un equipo de fútbol es muchas veces inevitable pensar que el gol se lo han metido al portero[1]. Si disponemos en nuestra infraestructura de sistemas de Protección y de sistemas de Detección+Respuesta, y un ataque logra hacer impacto, juéguense algo a que en la mayoría de los casos se culpará al último de no haber funcionado como debía, por esperarse de él una reacción infalible al ataque. El sistema de Protección (según la nomenclatura que estamos usando en este artículo) habrá funcionado bien en cualquier caso, pues su cometido no va más allá de la aplicación de unas reglas estáticas en las que nunca errará[2]. Así, cualquier sistema de Detección + Respuesta es firme candidato a resultar "chivo expiatorio".

En sus documentos técnicos y de tendencia de evolución de productos, cualquier fabricante de sistemas de perímetro o incluso de conectividad IP en general incluye entre sus "características" la "Prevención de Intrusiones".

Asociado al hecho de que estos sistemas tienen capacidad de respuesta desatendida está uno de los mayores "peros" que se ha achacado tradicionalmente a los sistemas de Detección + Respuesta. En algunos casos es posible provocar una respuesta del sistema que bloquee o degrade el mismo, haciéndole creer que está sufriendo un ataque. Un ejemplo sencillo de uno de estos ataques podría ser intentar bloquear una cuenta de acceso sobrepasando el número de intentos de autenticación permitidos. El sistema lo podría tomar como un intento de acceso no autorizado y bloquearía el ataque logrando el objetivo del atacante que es, en realidad, inhabilitar el acceso al usuario legítimo. Así, los primeros IDS con capacidad para resetear conexiones tuvieron un difícil comienzo

Tipo IPS *Producto*	Prevención o Protección *HIP*	Detección Respuesta *Detección + Respuesta*
Sistemas operativos bastionados	Pitbull Foundation de Argus Trusted Solaris de Sun eTrust Access Control de CA VirtualVault de HP	
Sistemas de control de acceso	Pitbull LX de Argus Stormwatch de Okena STAT Neutralizer de Harris Serverlock de Watchguard CylantSecure de Cylant Immunix de Wirex ...	
"Escudos" de servidores web	SecureIIS de eEye WebServer Edition de Entercept Applock de Watchguard Wavebraker de Pelican	
Cortafuegos para servidores web	AppShield de Sanctum HIVE de S21sec Interdo de Kavado DMZ/Shield de Ubizen	
IDS de pasarela		RealSecure Guard de ISS Intrushield de Intruvert IPS de Netscreen SmartDefense de Checkpoint Snort en línea Attack Mitigator de TopLayer ....

Figura 2.- Productos de IPS en el mercado.

[1] ¿Recuerdan los lectores/as sus partidos de fútbol a temprana edad? Siempre era difícil encontrar un portero voluntario, por estar éstos siempre predestinados a recibir goles y no marcarlos nunca.

[2] En los casos en los que se juega *sin portero*, esto es, sin sistemas de detección+respuesta, es inevitable cierta bronca a la *defensa* (sistemas de protección), aunque el pato lo pagará sin duda el entrenador, que siempre alegará falta de inversión del club para tener el equipo adecuado.

debido a que eran susceptibles de cortar conexiones inocuas.

En este proceso marco, ¿dónde encajan los sistemas que se venden actualmente de prevención de intrusiones? Para esto habría que analizar previamente que se han venido definiendo como sistemas de prevención de intrusiones. [LIND2002] propone la inclusión de los siguientes elementos dentro de la prevención de intrusiones, y de hecho, está basado en las aseveraciones de los fabricantes que los producen. Se muestra un resumen de productos y su ubicación en la **Figura 2**.

El objetivo del primer grupo (HIP) es proteger aún mejor los sistemas atacados, el objetivo del segundo es automatizar la respuesta que, habitualmente había dependido de una acción manual realizada por un administrador.

En qué quedamos: ¿qué es un IPS?

Claramente, una vez visto esto quizás la confusión del lector sea mayor. ¿A qué se le debe llamar correctamente IPS? Pues realmente la cosa no está nada clara, y la duda la tiene el sector y los propios profesionales como queda claro en [BIRM2002]. La realidad es que el término de *prevención de intrusiones* ha sido utilizado, de forma científica, en muy pocas ocasiones. Quizás la primera referencia que se pueda mencionar es [CPMHBBGWZ98], artículo que trata del uso de modificaciones del compilador para prevenir intrusiones en aplicaciones mediante la introducción de protecciones en éstas que prevengan contra los famosos errores de sobrecarga de búfer (que, recordemos, son más de la mitad de las vulnerabilidades habituales y que ya se conocen desde 1997) utilizando StackGuard (un producto de Wirex, creadores de Immunix que, por cierto, es software *libre*).

La utilización del término IPS ha surgido a la raíz de la popularización de la aparición de distintos productos con dicha "marca", desde el año 2002, enfocados a la resolución del problema actual de la mayor parte de las organizaciones: el servidor web, que es el punto más débil en la cadena de seguridad y por tanto hay que poner medios para protegerle específicamente. Estos nuevos productos, para distinguirse de la competencia, utilizaron nuevos términos. Así uno puede decir, "no, esto no es lo mismo que un FW o un IDS, esto es nuevo, es un IPS".

Nuestro vaticinio es que de aquí a unos años todos los fabricantes, sin ningún pudor ni rigor, dirán que sus sistemas son IPS, todas las herramientas tendrán esa "marca" y el término perderá cualquier utilidad que pudiera haber tenido.

Sin embargo, ya en las taxonomías de los sistemas de detección de intrusos se habla de la capacidad de detección de reacción automática frente a ataques como una cualidad más de un IDS [AXEL2000]. Recordemos que la detección de intrusos no es un área nueva, lleva desarrollándose 20 años, desde que apareciera el primer informe del Departamento de Defensa que trataba esta tecnología [AND1980].

En la actualidad, si los lectores echan un vistazo a los documentos técnicos y a las tendencias de evolución de productos, cualquier fabricante de sistemas de perímetro o incluso de conectividad IP en general incluye entre sus "características" la "Prevención de Intrusiones". Así Cisco, Enterasys, NetScreen, Watchguard, Fortinet, Symantec... Todos ellos están ampliando el alcance o funcionalidad de sus productos para que incluyan la detección y respuesta de ataques y por tanto, decir que se convierten en IPS.

También Gartner recientemente ha vaticinado (habrá que ver si con acierto) que los sistemas de detección de intrusión van a desaparecer [GART2002] y que la seguridad pasa por la introducción de sistemas de prevención [GART2003] que los sustituiran en el 2005, ya que los IDS no serán capaces de detectar los nuevos ataques. Claro, no tienen en cuenta de que la tecnología de IPS está, en algún caso, basada en la de IDS y ya muchos han levantado la voz en contra [HULME2003].

Nuestro vaticinio propio es que de aquí a unos años todos los fabricantes, sin ningún pudor ni rigor, dirán que sus sistemas son IPS, todas las herramientas tendrán esa "marca" y el término perderá cualquier utilidad que pudiera haber tenido. Sólo hay que ver la tendencia: antes sólo unos pocos decían que lo hacían, ahora todo el mundo dice que lo hace. ■

Antonio Requejo Novella
Director de la División de Seguridad
arequejo@germinus.com
Javier Fernández-Sanguino
Jefe de Proyecto
jfernandez@germinus.com
GERMINUS

REFERENCIAS

[AND1980] James P. Anderson: Computer Security Threat Monitoring and Surveillance <http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf>, James P. Anderson Co., Fort Washington, PA, 1980.

[CPMHBBGWZ98] "Automatic Detection and Prevention of Buffer-Overflow Attacks", Crispin Cowan, Calton Pu, David Maier, Heather Hinton, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, y Qian Zhang, el séptimo simposio de seguridad USENIX, San Antonio, Tejas, Enero1998.

[BIRM2002] What Isn't Intrusion Prevention? Andy Birney, InfoSecurity Mag. Abril 2002.

[HALBAU95] Ain't Misbehaving: a Taxonomy of Anti-Intrusion Techniques, L. R. Halme, y R. K. Bauer, publicado en Proceedings 18th National Information Systems Security Conference, 1995.

[AXEL2000] "Intrusion Detection Systems: A Survey and Taxonomy", Stefan Axelsson, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Suecia, marzo 2000.

[SCHNE2000] "Secrets & Lies. Digital Security in a Networked World", Bruce Schneier, John Wiley & Sons Inc, 2000.

[GART2002] Intrusion Prevention Will Replace Intrusion Detection, Richard Stiennon, Matthew Easley, agosto 2002.

[LIND2002] Guide to Intrusion Prevention, Pete Lindstrom, Information Security Magazine, octubre 2002. Una versión extendida de este artículo está disponible en http://www.spiresecurity.com/featured.asp

[GART2003] CIO Update: Enterprise Security Moves Toward Intrusion Prevention, John Pescatore y Richard Stiennon, IGG-06042003-03, junio 2003.

[HULME2003] Gartner: Intrusion Detection On The Way Out, George V. Hulme, Information Week, 13 de junio, 2003.